ABSTRACT OF THE DISCLOSURE

When electronic mail is to be sent by an off-line user to a recipient who holds a digital certificate, the sender's mail program allows the sender to compose the mail, but the mail is placed in plain text in the sender's local outbox and flagged for subsequent encryption. When the sender later connects to a mail server to send the outgoing mail, the sender's mail software, in response to the flagged mail will request the recipient's certificate from the server and use the received certificate to encrypt the mail message before it leaves the sender's workstation. In accordance with one embodiment of the invention, after using a digital certificate to encrypt a mail message, the certificate is discarded. In accordance with another embodiment, if the certificate is not available or located by the mail server, a message is sent to the sender informing him that the certificate cannot be located and the mail cannot be sent in encrypted form. At that point, the sender has an option to resend the mail in unencrypted form.